UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO

IN RE: SONIC CORP. CUSTOMER DATA SECURITY BREACH LITIGATION (FINANCIAL INSTITUTIONS)	CASE NO. 1:17-md-2807 MDL No. 2807 ORDER

JAMES S. GWIN, UNITED STATES DISTRICT JUDGE:

In 2017, unidentified third parties accessed Sonic[1] customers' payment card data. The hackers obtained customer payment card information from more than 300 Sonic Drive-Ins.

Plaintiffs, payment card issuing banks, sue Sonic Defendants for damages stemming from the 2017 data breach. Plaintiffs claim that the hackers accessed their customers' payment information during the breach and that Plaintiff banks suffered damages as a result of their steps to remediate the breach's effects.[2]

On October 28, 2019, Sonic moved to dismiss arguing that Plaintiffs fail to state a claim under Oklahoma law.[3] On November 25, 2019, Plaintiffs opposed.[4] On December 9, 2019, Sonic replied.[5] The Court held oral argument on December 18, 2019.

For the following reasons, the Court **GRANTS IN PART** and **DENIES IN PART** Sonic's motion to dismiss.

[1] Sonic Corporation and its subsidiaries and affiliates Sonic Industries Services, Inc., Sonic Capital LLC, Sonic Franchising LLC, Sonic Industries LLC, and Sonic Restaurants, Inc. (collectively, "Sonic" or "Sonic Defendants").

[2] Doc. 202 at 39-40.

[3] Doc. 199.

[4] Doc. 225.

[5] Doc. 226.

I. Background

When considering a motion to dismiss, the Court must accept the complaint's allegations as true and view the complaint in the light most favorable to Plaintiffs.[6]

Sonic restaurants are largely franchisee-owned. Sonic Defendants only directly own about 6% of Sonic restaurants.[7] However, Sonic exerts much control over the franchise restaurants, including the franchisees' data security policies.[8]

Plaintiffs allege that in 2015, Sonic's corporate-owned restaurants were hacked, and login credentials stolen.[9] The hackers attempted to install malware that would allow them to skim credit card data from Sonic's customers.[10] Sonic hired a third party data breach reviewer to investigate and remediate the threat.[11] After investigating the 2015 data breach, the third party reviewer warned that similar future attacks could occur. Despite this warning, Sonic did not address the described vulnerabilities.[12]

Despite the 2015 incident warning, industry-wide warnings, and many high-profile data breaches at other companies, Sonic continued to ignore industry security standards.[13]

Plaintiffs allege that Sonic largely controlled its franchisees' data security. Franchise agreements required franchisees to pay into a cybersecurity and technology fund that Sonic used to fund and control franchisees' security technology.[14]

Sonic's franchise agreements required Sonic franchisees conform to Sonic security

---

[6] *Toledo Elec. Welfare Fund v. Northwest Ohio Buckeye Elec., Ltd.*, 518 F. Supp.2d 1001, 1004 (N.D. Ohio 2007).

[7] Doc. 202 at 1.

[8] *Id.*

[9] *Id.* at 2-3.

[10] *Id.* at 3.

[11] *Id.*

[12] *Id.*

[13] *Id.* at 27-31.

[14] *Id.* at 14.

policies. Sonic and Sonic-approved vendors set up the technology that franchisees used, including preconfigured security settings.[15] Franchisees were not permitted to modify or change the security settings that Sonic corporate created.[16]

Sonic required franchisees to choose one of three Sonic-approved point of sale ("POS") technology vendors. Sonic disallowed using other vendors without express permission.[17]

As one of the three approved point of sale technology vendors, Sonic chose the card processing firm Infor. The 2017 breach locations all used Sonic-approved vendor Infor.[18]

In 2013, using the technology-fund money, Sonic updated its technology systems, including its point-of-sale technology.[19] Sonic alone selected the new technologies and the implementation timeline for each store.[20] However, at the time of the 2017 breach, 23% of Sonic locations still used the old technology. Sonic alone controlled the new technology roll-out and forbade franchisees from changing the technology.[21]

This made the franchise restaurants using the old technology vulnerable. For instance, Kitchen Display System, one system used by franchisees who had not received updated technology, had been "end of life" for almost a decade.[22]

In other words, the Kitchen Display System was so old that the system manufacturers had stopped updates and security patches almost a decade earlier.[23]

---

[15] *Id.* at 13-14, 21.
[16] *Id.*
[17] *Id.* at 13.
[18] *Id.* at 17.
[19] *Id.* at 14-15.
[20] *Id.*
[21] *Id.*
[22] *Id.* at 15-16.
[23] *Id.*

Additionally, this technology had no anti-virus or anti-malware software.[24] Plaintiffs allege that franchisees also used Windows XP operating systems, which had been end of life since early 2016, and Microsoft RDP, which was also outdated.[25]

In addition to the outdated hardware, Sonic required franchisees to maintain specific configuration settings, including a Sonic requirement that franchisees permanently enable remote access.[26] With remote access, Sonic—or hackers—could log in to the VPN and access the franchisees' cardholder data environments ("Cardholder Data").[27] Sonic also used weak passwords that required only 4 letters for VPN access.[28]

Starting on April 7, 2017, hackers breached Sonic's point-of-sale systems at the 762 Sonic franchisees that used the Infor system.[29] Sonic had created remote-access accounts for use by point-of-sale vendors, such as Infor.[30] Plaintiffs allege that "all Infor locations used the same non-complex, weak password to access the Kitchen Display Systems."[31] After obtaining legitimate Infor credentials, the hackers were able to access customer data in all Sonic restaurants that used the Infor platform.[32]

Access to the franchisees' point-of-sale system allowed the hackers to access the franchisees' Cardholder Data, the system that processes, stores, and transmits payment information for approval. The hackers installed malware on the stores' point-of-sale

[24] *Id.* at 16.
[25] *Id.*
[26] *Id.*
[27] *Id.* at 16-17.
[28] *Id.* at 22.
[29] *Id.* at 17.
[30] *Id.* at 21.
[31] *Id.* at 22.
[32] *Id.* at 20-21.

terminal or back-of-house servers through the end of life Kitchen Display System.[33] The malware allowed the hackers to access customers' credit card data.[34]

Plaintiffs allege that industry standard encrypts stored credit card data, but the hacked information was not encrypted because these stores used an outdated system for that portion of payment processing.[35] The hackers were able to obtain unencrypted payment card data in a form that allowed them to duplicate the stolen user information onto physical payment cards or make online purchases.[36] An investigation revealed that payment card data had been taken from the system and sold online.[37]

Hackers were able to siphon credit card data unabated for about six months, because Sonic had set up security alerts using an invalid e-mail address.[38] Because of this, Sonic only notified the public about the potential breach, about six months after it had begun.[39]

II. Discussion

As with all complaints, Plaintiffs' complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief."[40] When analyzing the complaint for a motion to dismiss under Rule 12(b)(6), the Court must be satisfied that the complaint "contain[s] sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'"[41]

---

[33] *Id.* at 21.
[34] *Id.*
[35] *Id.* at 19, 21.
[36] *Id.* at 21.
[37] *Id.* at 21-22.
[38] *Id.* at 16.
[39] *Id.* at 6, 20.
[40] Fed. R. Civ. P. 8(a)(2).
[41] *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)).

A. Count I- Negligence

In Count I, Plaintiffs allege that Sonic Defendants were negligent. They say that Sonic owed Plaintiffs and the proposed class a duty to secure data. Plaintiffs say they suffered damages from Sonic's failure to do so.[42] Sonic Defendants respond that Plaintiffs have not pleaded sufficient facts to show that Sonic had a duty under Oklahoma law.[43]

Under Oklahoma law, a negligence claim requires duty, breach, and causation.[44] Generally, Oklahoma law instructs that no duty is owed to another person to protect from third-party criminal acts.[45]

However, Oklahoma courts have recognized three special circumstances that can create a duty to anticipate and prevent a third party's foreseeable criminal acts[46]: (1) where the defendant is under a special responsibility toward the person harmed; (2) where the defendant's own affirmative act has created or exposed the other to a recognizable high degree of risk of harm through such misconduct, which a reasonable person would have taken into account; and (3) where the defendant has a special relationship to the person causing the injury.[47]

Here, the first and third circumstances are not applicable—the Sonic and the card-issuing Plaintiffs did not have a contractual relationship and Sonic had no relationship to the unknown criminal hackers.[48] The Court must therefore determine whether, under the

---

[42] Doc. 202 at 46-48.

[43] Doc. 199-1 at 7-18.

[44] *Lowery v. Echostar Satellite Corp.*, 160 P.3d 959, 964 (Okla. 2007).

[45] *J.S. v. Harris*, 227 P.3d 1089, 1092 (Okla. Civ. App. 2009).

[46] *Id.* at 1092-93 ("Oklahoma court have discussed special circumstances and special relationships as the bases for imposing liability on a defendant for the foreseeable harm a third person may inflict on another.").

[47] *BancFirst v. Dixie Restaurants, Inc.*, No. CIV-11-174-L, 2012 WL 12879, at *3-4 (W.D. Okla. Jan. 4, 2012) (citing *J.S.*, 227 P.3d at 1092-94).

[48] At oral argument, Plaintiffs conceded that the parties did not have a special relationship. Doc. 235 at 5.

second circumstance, Plaintiffs have sufficiently pleaded that Sonic's affirmative acts exposed Plaintiffs to a high degree of risk which a reasonable person would have considered. The Court finds that they have.

Plaintiffs argues that Sonic's affirmative acts exposed them to harm. They allege that Sonic controlled the franchisees' data security, that Sonic created and maintained remote access accounts that were permanently enabled and easily exploited, that Sonic required the franchisees to use security technology that was end of life or outdated, and that Sonic set up its security alerts to be sent to a defunct email address, delaying discovery of the card data breach. Defendants respond that Sonic might have *failed* to act, but it did not affirmatively create a risk.[49]

Oklahoma case law dealing with negligence liability when there are intervening criminal acts is not similar to this case.[50] Sonic's failure-to-act, as opposed to affirmative acts, argument relies heavily on *BancFirst*, the only case interpreting the Oklahoma's third-party-criminal-acts negligence case law in the context of a security data breach. In that case, BancFirst, an Oklahoma bank, sued Dixie Restaurants, which operated restaurants across several states, for damages resulting from the restaurants' data breach.[51] The federal district court granted the restaurant chain's motion to dismiss under Oklahoma law. In major part, the BancFirst district court dismissed the case because BancFirst did not allege

[49] Doc. 199-1 at 13-14.

[50] Many cases dealing with negligence claims involving intervening criminal acts concern liability for landlords or homeowners when a criminal act harms a tenant or house guest. *See, e.g., Brewer v. Murray*, 292 P.3d 41 (Okla. Civ. App. 2012). The other cases cited by the parties are not particularly instructive. For instance, in one, the court held that a fertilizer manufacturer did not commit affirmative acts under the standard by selling explosive grade fertilizer that was later used in a bomb. *Gaines-Tabb v. ICI Explosives USA, Inc.*, 995 F. Supp. 1304 (W.D. Okla. 1996). In another, the Tenth Circuit did not find a chemical manufacturer liable when an employee stole sulfuric acid and used it to harm someone. *Henry v. Merck and Co., Inc.*, 877 F.2d 1489 (10th Cir. 1989).

[51] *BancFirst*, 2012 WL 12879 (W.D. Okla. Jan. 4, 2012).

that the restaurant chain had taken affirmative acts that put the bank at risk.[52] Instead, BancFirst complained of the defendant restaurants' failure to put in place adequate security measures.[53] Despite the differences, the Sonic Defendants argue that the holding applies here.[54]

The Court disagrees with Sonic's argument that *BancFirst* requires the Court dismiss Plaintiffs' claims. As the *BancFirst* court noted, BancFirst's complaint largely dealt with the defendant Dixie Restaurants' failure to act.[55] Here, however, Plaintiffs have pleaded that Sonic Defendants affirmatively acted to create the vulnerabilities that the hackers easily exploited.[56] For instance, Sonic created the remote access accounts, required that they be kept open, created weak passwords, and set up security notifications to go to a defunct email account. All these acts, which Plaintiffs allege violated industry security standards, were affirmative steps taken by Sonic that put Plaintiffs at greater risk for suffering a data breach. The Court finds that at the motion to dismiss stage, this is enough to state a claim for negligence.

Sonic Defendants argue that their "[o]peration of a franchise business is not an affirmative act."[57] But while Sonic's operation of a franchise is not alone sufficient, the Sonic affirmative information technology decisions arguably led to the damages Plaintiffs complain of. Simply operating a franchise operation, alone, does not create liability. But some acts taken by the franchisor can create liability.

---

[52] *Id.* at *4.

[53] *Id.*

[54] Doc. 199-1 at 13-14.

[55] *BancFirst,* 2012 WL 12879, at *4 (W.D. Okla. Jan. 4, 2012).

[56] The present case is also distinguishable from the non-Oklahoma cases cited by Sonic, such as *Veridian Credit Union v. Eddie Bauer, LLC,* 295 F.Supp.3d 1140 (W.D. Wa. 2017), on the same grounds.

[57] Doc. 226 at 15-16.

In their reply, Sonic Defendants argue that Plaintiffs cannot show that a reasonable merchant would have considered the data breach risk associated with creating and maintaining the security measures the hackers later exploited.[58] However, the present case is distinguishable from *Gaines-Tabb*, on which Sonic heavily relies.

In that case, the plaintiffs alleged that the defendant fertilizer manufacturer was liable for injuries caused by a bomb detonated by a third party because the fertilizer manufacturer had distributed explosive grade ammonium nitrate on the fertilizer market. In *Gaines-Tabb* the plaintiffs argued that the fertilizer manufacturer should have manufactured a fertilizer grade with an additive that would prevent detonation.[59]

In finding that a reasonable person in the defendants position would have disregarded the risk of harm, the district court gave import to the allegation that ammonium nitrate had not been sold as ammonium nitrate but instead had actually been mislabeled and sold as fertilizer at a Kansas farmers' co-op.[60] The *Gaines-Tabb* Court also noted that the plaintiffs failed to plead that the defendant had reason to know of the criminal propensities of the farmers' co-op customers or that the bombers existed or planned to use the product in a bombing, much less that they planned to use the bomb against plaintiffs in Oklahoma.[61]

In comparison, in the present case Plaintiffs allege that Sonic had already suffered a similar data breach within years of this litigation's data breach.[62] Additionally, Plaintiffs say that there have been several high-profile data breaches, particularly within the fast food

[58] *Id.* at 9-12.
[59] *Gaines-Tabb*, 995 F. Supp. at 1317.
[60] *Id.* at 1317.
[61] *Id.* at 1317-18.
[62] Doc. 202 at 2-3.

industry, and that within the fast food industry, data experts had warned that hackers constantly look to breach data security systems.[63]

Although the *Gaines-Tabb* the court accepted the plaintiffs' allegations that defendants were aware that terrorists used bombs in bombing plots, the court found this allegation outweighed by the allegation that the ammonium nitrate was misbranded and sold as fertilizer at a farmers' co-op.[64] In this case, no similar mitigating factors exist reduce Sonic's knowledge of data breach risk.

Furthermore, the *Gaines-Tabb* court considered that the ammonium nitrate had been sold in Kansas but used in Oklahoma weighed against reasonable foreseeability.[65] However, despite Sonic's attempts to paint its connection to Plaintiffs as extenuated given Sonic Defendants' role as the franchisor and Plaintiffs' role as Sonic-franchise-store-customers' banks, Plaintiffs have pleaded sufficient facts to show that Sonic had reason to anticipate that cardholders' banks, which are responsible for replacing compromised cards and monitoring compromised accounts, could be harmed by any data breach.

Plaintiffs have pleaded sufficient facts to show that a reasonable person would have foreseen the data breach risk and its effects on Plaintiffs into account.

Finally, Oklahoma law incorporates foreseeability into the duty analysis.[66] In

---

[63] *Id.* at 27-31.

[64] *Gaines-Tabb*, 995 F. Supp. at 1318 ("Accepting as true all of Plaintiffs' allegations concerning Defendants' knowledge of terrorists' use of [ammonium nitrate] in bombs and bombing plots, but also considering as true Plaintiffs' allegations that the [ammonium nitrate] was branded as a fertilizer and sold through a farmers' cooperative in McPherson, Kansas, the recognizable possibility of risk of harm from Defendant ICI's distribution and sale of explosive grade [ammonium nitrate] through the intentional or criminal acts of third parties was so slight that reasonable persons in Defendant ICI's position would disregard it.").

[65] *Id.* ("Plaintiffs have not alleged and could not allege that Defendant ICI had any reason to know of the criminal propensities of customers of Mid–Kansas Cooperative Association, of the alleged perpetrators or of their intention to use Defendant ICI's product in a weapon of mass destruction, much less specifically against the Murrah Building and its occupants in Oklahoma City.").

[66] *See, e.g., J.S. v. Harris*, 227 P.3d 1089, 1092-93 (Okla. Civ. App. 2009) ("Oklahoma courts have discussed special circumstances . . . as the bases for imposing liability on a defendant for the *foreseeable* harm a third person may

general, criminal acts are "less foreseeable than negligent or intentional (but legal) acts," because "under ordinary circumstances it may reasonably assumed that no one will violate the criminal law."[67] However, as discussed above, Sonic Defendants had reason to assume, even anticipate, that many hackers would violate the law. Plaintiffs have pleaded sufficient facts to show that the data breach, even though caused by the criminal acts of a third party, was sufficiently foreseeable.[68]

The Court **DENIES** Sonic's motion to dismiss Count I of the amended complaint.

B. Count II- Negligence Per Se

In Count II, Plaintiffs bring a negligence per se claim based on violations of (1) Section 5 of the Federal Trade Commission Act, (2) the Oklahoma Consumer Protection Act, (3) the Oklahoma Breach Notification Act.[69] In their opposition to the motion to dismiss and at oral argument, Plaintiffs only respond to their FTCA Act negligence per se claim. Plaintiffs waived the Oklahoma law grounds.[70]

Plaintiffs negligence per se claim is therefore predicated solely on FTC Act Section 5, which declares unlawful any "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[71]

Under Oklahoma law, to state a negligence per se claim a plaintiff must show that "1) the injury was caused by the violation; 2) the injury was a type intended to be

---

inflict on another."); *Brewer*, 292 P.3d at 50 ("Foreseeability is often the primary policy consideration in defining the scope of duty in a particular case.").

[67] *Henry*, 877 F.2d at 1493 (citation and quotation omitted).

[68] *See, i.e.,* Doc. 202 at 2-3, 27-31.

[69] *Id.* at 49-53.

[70] *Notredan, LLC v. Old Republic Exchange Facilitator Co.*, 531 F. App'x. 567, 569 (6th Cir. 2013) (holding plaintiff forfeited a claim by failing to address the defendant's argument that plaintiff failed to state a claim under that count).

[71] 15 U.S.C. § 45(a).

prevented by the statute; and 3) the injured party was a member of the class which the statute was intended to protect."[72] In addition, Oklahoma courts have held that to support a negligence per se claim the underlying statute must "impose positive objective standards."[73]

The Court finds that because the FTC Act Section 5 does not lay out objective standards, it does not support a claim for negligence per se under Oklahoma law.

By its terms, the statute only prohibits unfair competition or unfair or deceptive acts. While the FTC and other courts have interpreted Section 5's terms to apply to data security requirements,[74] the statute's actual terms do not lay out positive, objective standards that, if violated, could give the standard for a negligence per se claim under Oklahoma law.[75]

Because FTC Act Section 5 cannot support a negligence per se claim, the Court **GRANTS** Sonic Defendants' motion to dismiss Count II.

C. The Economic Loss Rule

Sonic argues that even if Plaintiffs state a claim under their negligence theories, Oklahoma law still bars Plaintiffs' suit under the economic loss rule.[76] Under Oklahoma law, "[w]hen a party's loss is purely economic and does not entail personal or property damage, such losses have traditionally not been protected by application of tort law."[77]

---

[72] *Gaines-Tabb*, 995 F. Supp. at 1319.

[73] *Conway v. Lone Star Transportation, LLC*, No. 19-CV-0658-CVE-FHM, 2020 WL 609750, at *3 (N.D. Okla. Feb. 7, 2020) ("Oklahoma courts . . . hold that a positive objective standard is necessary for a negligence per se claim.") (citing *Wade v. Reimer*, 359 P.2d 1071, 1073 (Okla. 1961); *Smith v. Barker*, 419 P.3d 327, 333 (Okla. Ct. Civ. App. 2017)).

[74] *See Fed. Trade Comm'n. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247 (3d Cir. 2015); *In re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 498 (1st Cir. 2009), as amended on reh'g in part (May 5, 2009).

[75] *Chartney v. City of Choctaw*, 441 P.3d 173, 177 (Ok. Ct. App. 2019) (holding that regulation that "vaguely require[d] operators to properly operate and maintain facilities" could not sustain negligence per se claim for the discharge of pollutants into U.S. waters); *Conway*, 2020 WL 609750, at *3 (N.D. Okla. Feb. 7, 2020) (holding that driving "in willful or wanton disregard for the safety of persons or property" was not a positive objective standard).

[76] Doc. 199-1 at 19-20.

[77] *Compsource Oklahoma v. BNY Mellon, N.A.*, No. CIV-08-469-KEW, 2020 WL 2366112, at *2 (July 31,

The economic loss rule originated in products liability law, but many states have expanded the principle to other areas. Oklahoma is not one of them. Defendants do not cite any case, nor is the Court aware of one, in which Oklahoma courts applied the economic loss rule to stop recovery outside products liability litigation.[78] In fact, Defendants admit that Oklahoma has only applied the rule to bar purely economic recovery in products liability cases.[79]

Without Oklahoma case law extending the economic loss rule to non-products liability cases, Defendants urge the Court to look to the decisions of federal appellate courts applying other states' economic loss rules to similar factual circumstances.[80] However, none of these cases apply Oklahoma law, so they are inapposite here.

"If the state supreme court has not yet addressed the issue presented, we must predict how the court would rule by looking to all the available data."[81] Oklahoma federal courts addressing the same issue have declined to extend Oklahoma's economic loss rule outside the products liability context.[82] The Court finds no basis for predicting that Oklahoma's Supreme Court would hold differently.

The economic loss rule does not bar Plaintiffs' claims.

D. Declaratory and Injunctive Relief

Plaintiffs' Count III seeks declaratory and injunctive relief. The Federal Declaratory

---

2009).

[78] *See id.* ("No authority has been cited from a court in Oklahoma specifically adopting the economic loss rule outside of the products liability arena.").

[79] Doc. 199-1 at 25 ("[T]he Oklahoma Supreme Court has not expanded Oklahoma's economic loss rule beyond products liability cases. . . . ").

[80] Doc. 226 at 25.

[81] *Allstate Ins. Co. v. Thrifty Rent-A-Car Systems, Inc.*, 249 F.3d 450, 454 (6th Cir. 2001).

[82] *Compsource Oklahoma*, 2020 WL 2366112 at *2; *Lexington Ins. Co. v. Newbern Fabricating, Inc.*, No. 14-cv-0610-CVE-TLW, 2016 WL 4059251, at *6 (N.D. Okla. July 31, 2016); *Meier v. Chesapeake Operating LLC*, 324 F. Supp. 3d 1207, 1217 n.6 (W.D. Okla. 2018).

Judgement Act provides the Court with discretion to "declare the rights and other legal relations of any interested party seeking such declaration" where there is an "actual controversy."[83] However, declaratory judgment is a remedy or the relief sought, rather than an independent cause of action.[84] While Plaintiffs may continue to seek declaratory relief based upon their surviving claim, it does not constitute a separate cause of action.

Likewise, Plaintiffs may seek injunctive relief, but it does not provide a substantive cause of action.[85]

The Court dismisses Count III to the extent that it purports to bring an independent cause of action based solely on declaratory or injunctive relief.

III. Conclusion

For the foregoing reasons, the Court **DENIES** Sonic Defendants' motion to dismiss Count I and **GRANTS** Sonic Defendants' motion to dismiss Counts II and III.

ITS IS SO ORDERED.

Dated: July 1, 2020

s/ James S. Gwin
JAMES S. GWIN
UNITED STATES DISTRICT JUDGE

[83] 28 U.S.C. § 2201.

[84] *Duncan v. Tennessee Valley Authority Retirement System*, 123 F. Supp. 3d 972, 982 (M.D. Tenn. 2015), *affir'd in part* by *Duncan v. Myzyn*, 833 F.3d 567 (6th Cir. 2016) ("Declaratory judgment . . . is not a cause of action, but a specific type of relief."); *Jones v. ABN AMRO Mort. Group, Inc.*, 551 F. Supp. 2d 400, 406 (E.D. Pa. 2008) ("Declaratory judgment is a remedy, not a count."); *Kimball v. Flagstar Bank F.S.B.*, 881 F. Supp. 2d 1209, 1219 (S.D. Cal. 2012) ("Declaratory relief is not an independent cause of action, but instead a form of equitable relief.").

[85] *Goryoka v. Quicken Loans,* 519 F. App'x. 926, 929 (6th Cir. 2013) (holding that the district court properly dismissed a claim for injunctive relief, because the injunctive relief is a remedy, not a separate cause of action).